Seqrite Endpoint Security 7.6

Release Notes

Copyright Information

Trademarks

License Terms

Installation and usage of Seqrite Endpoint Security is subject to user's unconditional acceptance of the Seqrite end-user license terms and conditions.

To read the license terms, visit http://www.seqrite.com/eula and check the End-User License Agreement for your product.

Contents

Introducing Seqrite Endpoint Security

For every organization, security of valuable data and resources is of paramount concern. Today, Web technology is an integral part of business processes for all organizations. This puts them more at risk from new and unknown threats and attacks. Seqrite Endpoint Security (SEPS) is designed to provide complete security solutions to small and enterprise-level networks against various kinds of malicious threats such as; viruses, Trojans, worms, backdoors, spyware, riskware, adult content, and hackers.

SEPS is a Web-based management solution that integrates desktops, laptops, and network servers. It allows you to access all clients and servers in the network and manage them remotely. You can deploy antivirus software applications, configure security policies, signature pattern updates, and software updates on the clients and servers. You can also monitor clients to check whether there are any policy breaches or security threats within the organization and take appropriate actions for ensuring security across the networks.

How Does Seqrite Endpoint Security Work?

Seqrite Endpoint Security (SEPS) works on the Client/Server architecture where the console manages all the client agents deployed on the network. The console and client agents can be installed on almost all flavors of Microsoft Windows operating systems. The client agents can also be installed on the machines with Linux and Mac operating systems. For a detailed description of console and client agent system requirements and compatibilities, see System Requirements.

SEPS helps the administrators deploy Seqrite Antivirus remotely on the specified computers, groups or domains, which are part of the same domain. Whenever the server copy of Seqrite Antivirus is updated, all computers configured to update from the server will be automatically updated without user intervention. SEPS monitors these processes so that an administrator can view the computers that have Seqrite Antivirus installed, the virus database date of Seqrite, whether Virus Protection is enabled, and if viruses are active in the memory of workstations. If any virus is found active in the memory of a workstation, that workstation gets disconnected from the network. If it detects that Seqrite is uninstalled from any workstation(s), it reinstalls Seqrite remotely without user intervention. This keeps the computers and the network safe from virus threats.

Available flavors

Seqrite Endpoint Security is available in the following flavors:

- SME (Small and Medium Enterprises Edition)
- Business

- Total
- Enterprise Suite

More Information

For information on the installation and system requirements of Seqrite Endpoint Security, refer to the Administration Guide.

For more information about the product and Data sheet, visit

https://www.seqrite.com/seqrite-endpoint-security

New Features and Enhancements

Windows Client Build released on 23 March 2022

- The build is prepared for the following bug fix.
    - EPS client installation is getting failed on Windows XP Operating System.
- Latest engine files are included in this build.

Mac Client Build released on 16 March 2022

- Mac client provides support to Apple's M1 chip.
- Latest engine files are included in this build.
- IMPORTANT:

  AV updates released on 8 March 2022 should be applied on Seqrite EPS 7.6 Server before installing this Mac build on the Mac system.

  If latest AV updates are not applied, Mac client will not take updates from the Endpoint Security Server and the following error message appears, 'Definition files not found'.

Mac Client Build released on 03 February 2022

- Mac client compatibility with macOS Monterey 12.
- Latest engine files are included in this build.

Build 7.6 released on 01 December 2021

- Endpoint IP Address details included in IDS/IPS, Port Scan and DDoS Report.
- Local and Remote Port details included in the Firewall Report.
- Complete Asset details of all endpoints can be exported in a single report from EPS web console > Clients > Assets > Download Complete Asset Details button.
- Endpoint Name and IP Address details included in SMS Notification for Virus and Ransomware attack.
- Option to configure OCR and File Fingerprinting settings added in EPS web console > Settings > Data Loss Prevention (DLP).
- Enhancement in client deployment method through Active Directory to support enumeration of large number of objects (10,000) in Active Directory while synchronizing Active Directory.

- Patch Management reports section now contains additional reports for Up-to-date, Patch Scan failed, and Patch Installation failed endpoints. Earlier only Missing and Installed patches reports options were available.
- The default applications listed in Application Control feature will be updated automatically to the latest version. The latest application version signatures will be released periodically through AV updates.
- Upgrade support is added for Windows 10 operating system through Seqrite Patch Management.
  - Configure Seqrite Patch Server to get upgrade patches for Windows 10 operating system from “Seqrite EPS Web console > Admin Settings > Server > Patch Management > Configure Patch Server > Filters” page.
  - In the Products tab, under Microsoft > Windows, select “Windows 10” and “Windows 10, version 1903 and later” and In the Categories tab, select the “Upgrades”.
- Consolidated Dashboard and Manage Secondary Server tabs will not be visible on EPS web console dashboard if EPS server does not have Secondary EPS server.
- On EPS dashboard top 10 incident count will be displayed instead of top 5. The top 10 incident can be exported to csv report.
- Notifications are displayed on browser if any website is blocked by Web Security feature. Earlier only alert messages used to appear. This feature is applicable only for clients installed on Windows platform.
- EPS server compatibility with Windows 10 21H2, Windows 11 and Windows Server 2022. (Now IIS will be installed automatically, Correct OS name will appear in info.qhc).

  Note:

  - If Master EPS Server installed on Windows Server 2022 and Windows 11 then, Secondary Server and Patch Management server installed on Windows 7, Windows Server 2008 and lower operating system fails to communicate with Master EPS server.
    - Secondary Server console is not able to connect from Master Server EPS web console > Manage Secondary Servers > Status of Secondary Servers > Go to Server.
    - Patch Management server is not able to add from EPS web Console > Admin Settings > Server > Patch Management > Add New Patch Server. It shows an error message ‘Patch server is unreachable. Please try later’.

  Seqrite recommends to install Secondary Server and Patch Management server on the higher version OS.

Mac Client Build released on 17 March 2021

- The following known issues in the 'Mac Client Build released on 13 November 2020' are fixed.
  - Data Loss Prevention

    Data transfer through clipboard and Application/Online Services will not be monitored and blocked on macOS Big Sur.
  - File Activity Monitor reports may not be generated in certain cases for clients installed on macOS 10.15 and above.
  - If the client is deployed remotely when no user is logged in to the system on macOS 10.15 or above, the 'webflt' prompt appears after system restart.
- To enable Virus Protection, you need to allow 'opsext' system extension in System Preferences > Security & Privacy > Full Disk Access.

  Earlier system restart was required after allowing 'opsext' from Full Disk Access.
  Now system restart is not required to activate Virus Protection.
- Latest engine files are included in this build.

Linux Client Build released on 30 November 2020

- TLS support binaries: accaadv.ini (connectionmodetls), cspsock.so, bfafv.dat
  - Now, with the updated binaries, the client-server socket communication will be established over TLS. Earlier client-server socket communication used to be established over SSL.
- Latest engine files are included in this build.

Mac Client Build released on 13 November 2020

- Mac client compatibility with macOS Big Sur 11.0.
- Latest engine files are included in this build.

Build 7.6 released on 13 July 2020

- Windows, Mac and Linux client AV builds are integrated with latest engine.
- Service Pack 3 bug fixes/enhancements are included.
- Roaming Platform (RP) optimization for service pack (SP): Earlier client service pack files were uploaded to the RP server from every EPS server. This used to consume lot of disk space.

Now, these client service pack files are maintained on a centralized location, Example: http://download.quickheal.com/. EPS server will send the centralized location of the service pack to the roaming clients to apply SP.

- EPS server compatibility with Windows 10 20H1 - 32 bit/64 bit.
- Mac client compatibility with macOS 10.15.4.
- Linux client compatibility with CentOS version 7.4, 8.0 and 8.1.
- Samba version support for 4.10 and 4.11.

Build 7.6 released on 26 Aug 2019

- Master and multi-level secondary server architecture - As per your geographical locations, multiple and multi-level secondary servers are possible as per your requirement.
- EPS server compatibility with Windows 10 RS5 - 32 bit/64 bit.
- EPS server supports MySQL 5.6.42 version.
- Asset Management feature displays following additional info,
    - OS Product key
    - Software upgrade changes in Reports and Dashboard
- Provision to exclude MD5 from Scan Settings. To do this, go to Settings > Scan Settings > Exclusion.
- In the Scan Settings > Advance > Archive Scan Level, Archive Scan Levels supports up to 16 levels.
- Provision to block/deny all URLs in the Web security feature with single button.
- The License Manager page shows additional details of license usage regarding Master/Secondary server and DLP licenses as applicable.
- Hierarchy representation of Server name on EPS Dashboard

  On the Master server, “Hierarchy” name will be represented as “Master”.

  On the Secondary Server, displays the hierarchy of the Server you have logged-on. This shows the names of the parent servers up to Master. Example: Master / Primary001 / Secondary001. In this case, the logged-on Server name is Secondary001 and the parent Server is Primary001, which is reporting to the Master.
- Displays online/offline status of Secondary Server on the Dashboard > Manage Secondary Server. The Green dot indicates online status. The Red dot indicates offline status. If the last connected time of Secondary server with the Master/parent server exceeds 2 hours, the status will be shown as offline.
- Centralized Policy Deployment
- On the Master server, the administrator will assign a policy for the Secondary Server. This policy is applied to the Secondary Server, its endpoints till the leaf Secondary Server. On the Secondary Server, this policy is not allowed to modify.

- Provision to add Multiple IP addresses and DNS names (URL) in exception of Seqrite Firewall.
- GDPR - General Data Protection Regulation check box added on Software License Agreement.
- Displays VDB date along with Update time [hh:mm: ss] on Windows, Mac and Linux Client Scanner and on EPS Web Console.
- Provision to lock license with respect to country. The EPS License should be functional only in the specified countries.
- Provision to select all Patches at once for specific endpoints.
- Provision to store data backup in a customized way. You can add custom extensions to the custom list. Provision for customized backup reports.
- Authorized USB can be accessed in different EPS networks if administrator export policy with authorized USB settings and import into different EPS networks.
- On 64-bit Linux operating system - Linux Client AV GUI is now supported.
- When Master admin logs on Secondary server via auto login, then Master admin activity logs will be generated in Secondary sever event logs.
- Included latest 'Remote Support Tool - Team Viewer version (14.1.18533 QSC)' in Windows client AV builds.
- As a part of branding, added logo for GoDeep.AI on EPS console footer.

Known Issues

Mac Client Build released on 16 March 2022

Mac Client

- The following features are not supported on Apple's M1 chip.
  - Advance Device Control
  - Spam Protection
- On the macOS 11.5.x system, the following issues may occur.
  - Data Loss Preventions (DLP) extensions may get unloaded.
  - Apple Mail application may not be launched if Data Loss Prevention (DLP) is enabled and in the Confidential Data tab, the 'Personal' check box is selected.

  Upgrade to macOS 11.6 to resolve these issues.
- Email Protection will not work if SSL/TLS setting is ON at Mail application.

  This issue occurs in macOS M1 chip and macOS Monterey 12 and above.

  How to verify SSL/TLS settings

  SSL/TLS Settings are available at different location for different Mail clients.

  Examples:

  - Apple Mail Application:
    a. Open Mail application.
    b. Select your Email account.
    c. In the Server Settings tab, clear the 'Automatically manage connection settings' check box and verify TLS/SSL settings.
  - Thunderbird:
    a. Open Thunderbird application.
    b. Select your Email account.
    c. Go to Account settings > Select Server Settings. Verify SSL/TLS settings under Security Settings.
- Bluetooth blocking functionality does not work on macOS Monterey 12, though Device Control Blocked prompt appears.

- If the Mac system is kept unlocked and in idle state for 2-3 days, the Client Dashboard does not launch. The policy status is also shown as Pending on the EPS Server Web Console, Client > Manage Policies page. Restart the system to resolve this issue.
- While scanning, if the scan is initiated on One Drive folder as per scan sequence, scanning does not progress/continue. The Client Dashboard also does not respond.
- Asset Management
    - On the Asset Management Reports page, in the Current Assets tab, in the 'Operating System' drop down list, 'macOS Monterey' name is displayed as blank space. If you select the blank space, the respective data appears with Mac OS name.
    - On the EPS Dashboard, if you select Asset > Platforms > Mac, macOS Monterey details are displayed under the 'Big Sur' bar chart.

Mac Client Build released on 03 February 2022

Mac Client

- The Apple M1 chip is not supported.
- On the macOS 12.x system, the following issues may occur.
    1. Bluetooth blocking functionality does not work on macOS Monterey 12, though Device Control Blocked prompt appears.
    2. Email Protection will not work if SSL/TLS setting is ON at Mail application.

       How to verify SSL/TLS settings

       SSL/TLS Settings are available at different location for different Mail clients. Examples:
        - Apple Mail Application:
            a. Open Mail application.
            b. Select your Email account.
            c. In the Server Settings tab, clear the 'Automatically manage connection settings' check box and verify TLS/SSL settings.
        - Thunderbird:
            a. Open Thunderbird application.
            b. Select your Email account.
            c. Go to Account settings > Select Server Settings. Verify SSL/TLS settings under Security Settings.

3. Asset Management
    - On the Asset Management Reports page, in the Current Assets tab, in the ‘Operating System’ drop down list, 'macOS Monterey' name is displayed as blank space. If you select the blank space, the respective data appears with Mac OS name.
    - On the EPS Dashboard, if you select Asset > Platforms > Mac, macOS Monterey details are displayed under the ‘Big Sur’ bar chart.

Build 7.6 released on 01 December 2021

Mac Client

- The macOS Monterey and Apple M1 chip is not supported.
- On the macOS 11.5.x system, the following issues may occur.
    - Data Loss Preventions (DLP) extensions may get unloaded.
    - Apple Mail application may not be launched if Data Loss Prevention (DLP) is enabled and in the Confidential Data tab, the 'Personal' check box is selected.

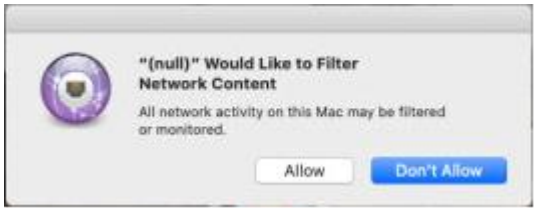
  Upgrade to macOS 11.6 to resolve these issues.
- While scanning, if the scan is initiated on One Drive folder as per scan sequence, scanning does not progress/continue. The Client Dashboard also does not respond.

Mac Client Build released on 13 November 2020

Mac Client

- Data Loss Prevention

  Data transfer through clipboard and Application/Online Services will not be monitored and blocked on macOS Big Sur.
- If the client is deployed remotely when no user is logged in to the system on macOS 10.15 or above, the following prompt appears after system restart. Click **Allow** to allow ‘webflt’ system extension.



  If you click **Don’t Allow**, you need to generate the above prompt manually by executing the following command:

  ```
  /Applications/webflt.app/Contents/MacOS/webflt -start
  ```

  After executing the command, the prompt appears. Click **Allow**.

- File Activity Monitor reports may not be generated in certain cases for clients installed on macOS 10.15 and above.

Technical Support

Seqrite provides extensive technical support for the registered users. It is recommended that you have all the necessary details with you during the call to receive efficient support from the support executives of Seqrite.

The Support option includes FAQ (Frequently Asked Questions) where you can find answers to the most frequently asked questions, options to submit your queries, send emails about your queries, or call us directly.

To access the Support options, follow these steps:

1. Log on to Seqrite Endpoint Security Web console.
2. On the top right on Seqrite Endpoint Security Dashboard, click the **Support** button.

Support includes the following options:

Web Support: Includes **Visit FAQ** (Frequently Asked Questions) and **Visit Forums** – where you can submit your queries to get an appropriate answer.

Email Support: Includes **Submit Ticket** that redirects you to our Support webpage. Here you can read some of the most common issues with answers. If you do not find an answer to your issue you submit a ticket.

Live Chat Support: Using this option, you can chat with our support executives.

Phone Support: Includes phone numbers. You can call our support team and get your issues resolved.

Remote Support: This support module helps us easily connect to your computer system remotely and assist you in resolving technical issues.

The Remote Support feature is available in the clients with Microsoft Windows, Mac, and Linux operating systems.
Remote support feature does not support the Linux clients connected through 'PuTTY' or using an OS without GUI.

Support by Phone

Contact number for phone support: 1800 212 7377

To know more phone numbers for support, please visit
http://www.seqrite.com/contact_support

Other sources of support

To get other sources of support, please visit:

http://www.seqrite.com/seqrite-support-center

If the Product Key is Lost

Product Key serves as your identity to your Seqrite Endpoint Security product. If you lose the Product Key, please contact Seqrite Technical Support to get the Product Key. A nominal charge is levied for re-issuing the Product Key.

Head Office Contact Details

Quick Heal Technologies Limited

(Formerly known as Quick Heal Technologies Pvt. Ltd.)

Reg. Office: Marvel Edge, Office No.7010 C & D, 7th Floor,

Viman Nagar, Pune 411014, Maharashtra, India.

Official Website: http://www.seqrite.com.

Email: support@seqrite.com